Statement of
Scott I. Aaronson
Senior Director, National Security Policy
Edison Electric Institute

Before the
Energy and Technology Committee
Michigan State Senate

December 10, 2013

My name is Scott Aaronson, and I am the Senior Director for National Security Policy at the Edison Electric Institute (EEI).

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly employ more than 500,000 workers. EEI has 70 international electric companies as Affiliate Members, and 250 industry suppliers and related organizations as Associate Members. EEI member companies that serve Michigan customers include CMS Energy Corporation, DTE Energy Company, Integrys Energy Group, ITC Holdings Corporation, and Wisconsin Energy Corporation. On behalf of all of EEI's members, I appreciate your invitation to discuss the cybersecurity of critical electric infrastructure.

EEI's member companies—along with other owners, operators, and users of the electric grid—take cybersecurity threats seriously and are committed to making cybersecurity a priority. In fact, EEI is part of a broader coalition of electric power stakeholders working together to make our critical infrastructure more resilient. While I am not officially testifying on its behalf, this coalition includes several major trade associations representing the full scope of electric generation, transmission, and distribution in the United States, as well as regulators, Canadian interests, and large industrial customers. Rarely do these groups find consensus on public policy issues, but in the case of securing the electric grid, there is unanimous support for a regime that leverages the strength of both the public and private sectors to improve cybersecurity. My testimony focuses on the value of this cooperative relationship, the public policy considerations for addressing cyber threats to critical infrastructure, and the ongoing efforts of the nation's electric sector to respond to those threats.

Cybersecurity for Critical Infrastructure:
Industry-Government Partnerships and Interdependencies

Cybersecurity can mean many things, so for the purposes of my testimony I want to be clear that my focus is on operational threats to critical assets. That is not to diminish the importance of protecting business systems and customers' data; however, my focus today is less on economic crimes and cyber breaches, and more on threats to national security from adversaries seeking to disrupt the flow of electricity.

General Michael Hayden, former Director of both the Central Intelligence and National Security Agencies, calls "cyber" the fifth domain of warfare. That is, in addition to the traditional theaters of war—air, land, sea, and space—we now have a fifth domain to defend. Whether as a precursor to war, an act of terrorism, ongoing espionage, or for economic gain, we know our adversaries are pursuing capabilities to attack, manipulate, or disable assets across the critical infrastructure sectors through cyber means. Complicating factors in the defense of critical infrastructure are that so many of these potential targets are owned and operated by the private sector, and that many of the sectors are interdependent.

On the issue of private-sector ownership of critical assets, government and industry must work closely and leverage each other's expertise. The electric power sector does not have intelligence-gathering capability or military forces; we need the government to help identify threats and provide technological support to assist in the defense of our systems. Similarly, the government does not have the experience to operate an electric utility system; it must depend on the engineering and operational expertise that keeps the grid running reliably in the face of all hazards.

With respect to interdependence, the electric power sector often is described as the most critical of the critical infrastructure sectors. And while it is true that the other critical sectors depend on a reliable supply of electricity for their operations, the electric power sector is dependent on them as well. EEI's member companies need water to cool their systems and to create steam that spins generating equipment. They need telecommunications to operate the grid. And they need transportation and pipeline systems to move the fuel they use.

Given these factors, it is increasingly apparent that no single entity can be solely responsible for the protection of critical infrastructure. Instead, we must leverage private-sector expertise from across the critical infrastructure sectors, from the military and intelligence communities, and from law enforcement and homeland security experts at both the federal and state levels.

Managing Cyber Risks:
What are the risks to the electric power sector?

Risk often is framed as the threats a system faces, the consequences of a successful attack, and the vulnerability or susceptibility to such an attack. This is distilled into the "risk equation":

Risk = Threat x Consequence x Vulnerability

By assessing risk using this formula, electric utility operators and our government counterparts are able to understand the nature of the threats we face, the roles and responsibilities that both government and industry play in mitigating these threats, how best to prioritize protection, and where more can be done to further reduce risk exposure.

What is the cyber <u>threat</u> to the electric power sector?

Threats are best discussed in terms of the capabilities of our adversaries and their intent. Of the "millions of attacks" we are told happen each day, the intent behind nearly all of them is economic crime: exfiltration of data, corporate espionage, theft of information, or network vandalism. These attacks are serious in their own right, but they do not have the same impact on national security as an attack on an industrial control system might.

Only a very small number of attacks are focused on the computer networks responsible for generating, transmitting, and distributing power across the electric grid. Known as industrial control systems and Supervisory Control and Data Acquisition (SCADA) systems, the level of sophistication required to attack these networks is high, and the adversaries capable of perpetrating such attacks are few.

That said, we recognize that a threat actor's sophistication is not static, and that there is intent by some adversaries to target the electric power sector's operational controls. Just as our ability to defend systems improves, the capabilities of our adversaries are constantly evolving, too. This speaks to the value of close coordination with the intelligence community and law enforcement; constant monitoring of our computer networks and our adversaries' capabilities helps ensure operators of critical infrastructure are focusing their resources appropriately.

What are the consequences of an attack that impacts electric service?

The electric power sector is deemed "critical infrastructure" because it is critical to national security and to maintaining social order. This is a responsibility that the industry takes very seriously. We understand that a successful attack could have very serious impacts for the economy, and for the life, health, safety, and protection of American citizens.

In fact, given the industry's experiences in dealing with the consequences of power disruptions from natural disasters, resiliency is a key focus of the grid's engineering. The very nature of the grid, specifically the redundancy and "biodiversity" that have been introduced over decades, makes an attack with widespread, long-lasting effects very difficult to perpetrate.

But, as with anything, the likelihood of an attack resulting in consequences for the grid can never be "zero," so we continue to work closely as an industry and with our government partners to prepare for worst-case scenarios and to make restoration and recovery as quick as possible.

How are electric utilities managing vulnerabilities?

This is the portion of the risk equation that the industry has the greatest ability to affect. Threats and consequences must be managed, but vulnerabilities can be actively mitigated to reduce risk.

The "millions of attacks" a day referenced earlier are essentially the car thieves looking for unlocked doors as they walk down the street. By simply locking your car door—eliminating a vulnerability—you can deprive a thief of an easy target. This is something the electric power sector has done by adopting Critical Infrastructure Protection (CIP) standards. These CIP standards are both mandatory for all owners and operators of Bulk Power System assets, and enforceable by the Federal Energy Regulatory Commission (FERC) with fines of up to $1 million per day.

As valuable as the CIP standards are in ensuring basic network hygiene and baseline levels of security for the thousands of entities operating the electric grid, they alone cannot account for the very dynamic nature of cyber risks.

Instead, the electric power sector has seen the value both of implementing CIP standards *and* of developing close working relationships with federal and state governments. These strategic partnerships help to identify vulnerabilities that could be exploited, implement defenses quickly based on the ever-changing threat environment, and respond in a coordinated way to any successful attacks.

In addition to working together as a sector in common defense of the electric grid, the industry's recent work with government partners has provided a significant boost to cyber preparedness.

Government-Industry Partnerships: *Electricity Subsector Coordinating Council (ESCC)*
As has been noted throughout this testimony, protection of critical infrastructure is a shared responsibility between the government and industry. The ESCC was formed to help coordinate these efforts and to ensure we are appropriately deploying each other's expertise, capabilities, and assets. The group is made up of utility CEOs and trade association leaders representing all segments of the industry, actively partnering with government executives to prepare for, and respond to, national-level disasters or threats to the electric grid.

In meetings with senior government leaders over the last year, the ESCC has focused its efforts on three areas of industry-government collaboration:

1. Incident Response: planning and exercising to coordinate responses to an attack

2. Information Flow: making sure actionable intelligence and threat indicators are communicated to the right people at the right time

3. Tools & Technology: deploying the proprietary government technologies that enable machine-to-machine information sharing

The key value of the ESCC is the executive engagement. In addition to providing resources and accountability that have pushed both the government and industry to work very closely and very quickly, senior executives on both sides also help to ensure unity of effort among their organizations. Further, these senior executives help to ensure a coordinated response, appropriate prioritization and allocation of resources, as well as support for deviation from standard procedures during an incident.

The establishment of the ESCC has been invaluable, providing a primary liaison for government entities and other sectors to partner at the senior-executive level with the electric utility industry.

Conclusion

On behalf of owners and operators of critical electric infrastructure, I appreciate the Committee holding this hearing to learn more about cyber threats facing the industry. It is my hope that this testimony provides insight into what the electric utility industry is doing to address these threats, but also to make it clear that there is no such thing as risk elimination, only risk management.

As we work to manage risks facing the sector and the nation, I believe these efforts must be a shared responsibility between the owners and operators of critical infrastructure and our government partners. I am proud to say the electric power sector and the government are working closely together in innovative ways to protect critical infrastructure from attacks and also to limit the consequences of an attack should one occur.

Thank you again for the opportunity to appear today, and I would be happy to answer any questions for the record.